(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－47912
（P2000－47912A）
(43)公開日　平成12年２月18日(2000.2.18)

(51)Int.Cl.'	識別記号	Ｆ Ｉ	テーマコード'(参考)
Ｇ０６Ｆ　11/34		Ｇ０６Ｆ　11/34	Ｓ　５Ｂ０４２
Ｈ０４Ｌ　12/24		Ｈ０４Ｌ　11/08	５Ｋ０３０
12/26			

審査請求　未請求　請求項の数３　ＯＬ　（全６頁）

(21)出願番号　特願平10－215989

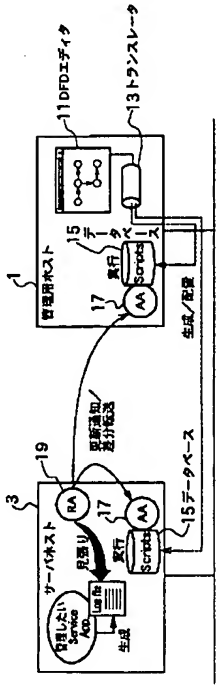
(22)出願日　平成10年７月30日(1998.7.30)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　犬束　敏信
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　浜田　雅樹
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外１名）

Ｆターム(参考)　5B042 GA09 GA19 GB03 JJ17 KK13
LA19 MA14 MC40
5K030 GA16 HA06 HB08 JA10 MC08

(54)【発明の名称】　ネットワークサービス監視方法および装置とネットワークサービス監視プログラムを記録した記録媒体

(57)【要約】
【課題】　管理者の負担を軽減しながら異常状態を迅速に対応してネットワークサービスの監視を適確に行い得るネットワークサービス監視方法および装置とネットワークサービス監視プログラムを記録した記録媒体を提供する。
【解決手段】　管理用ホスト１のデータフロー図エディタ１１でログ情報の解析手順をデータフロー図で記述し、該データフロー図をトランスレータ１３で監視プログラムに生成し、該監視プログラムをスクリプトデータベース１５に記憶する。サーバホスト３の監視エージェント（ＲＡ）１９によりサービスが生成するログ情報を監視し、ログ情報の変化を検出すると、解析エージェント（ＡＡ）１７はログ情報の変化の検出に応答し、監視プログラムを実行し、この結果をテキストファイル、電子メール等の指定された方法で出力し、管理者に通知する。



【特許請求の範囲】
【請求項1】 電子メール、ネットニュース、WWWを含むネットワークサービスが提供されているネットワークに接続された電子計算機環境において、
前記ネットワークサービスが生成するログ情報を逐次監視して、ログ情報の変化を検出し、
ログ情報の解析手順をデータフロー図で記述して、監視プログラムを生成し、
この生成した監視プログラムを配置し、
前記ログ情報の変化を検出した場合、前記生成され配置された監視プログラムを実行し、これによりネットワークサービスを監視することを特徴とするネットワークサービス監視方法。
【請求項2】 電子メール、ネットニュース、WWWを含むネットワークサービスが提供されているネットワークに接続された電子計算機環境において、
前記ネットワークサービスが生成するログ情報を逐次監視して、ログ情報の変化を検出するログ情報変化検出手段と、
ログ情報の解析手順をデータフロー図で記述して、監視プログラムを生成する生成手段と、
この生成した監視プログラムを配置して記憶するデータベース手段と、
前記ログ情報変化検出手段がログ情報の変化を検出した場合、前記データベース手段に記憶された監視プログラムを実行し、これによりネットワークサービスを監視する監視プログラム実行手段とを有することを特徴とするネットワークサービス監視装置。
【請求項3】 電子メール、ネットニュース、WWWを含むネットワークサービスが提供されているネットワークに接続された電子計算機環境において、
前記ネットワークサービスが生成するログ情報を逐次監視して、ログ情報の変化を検出し、
ログ情報の解析手順をデータフロー図で記述して、監視プログラムを生成し、
この生成した監視プログラムを配置し、
前記ログ情報の変化を検出した場合、前記生成され配置された監視プログラムを実行し、これによりネットワークサービスを監視することを特徴とするネットワークサービス監視プログラムを記録した記録媒体。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、電子メール、ネットニュース、WWW (World Wide Web) を含むネットワークサービスが提供されているネットワークに接続された電子計算機環境においてネットワークサービスが正常に作動しているかどうかを監視するネットワークサービス監視方法および装置とネットワークサービス監視プログラムを記録した記録媒体に関する。
【0002】
【従来の技術】昨今のインターネット、イントラネットの興隆により、電子計算機環境における電子メール、ネットニュース、WWWといったネットワークサービスは不可欠なものとなってきている。ネットワークサービスを滞りなく提供するためには、個々のサービスが正常に動き続けていることを定常的に確認し、かつ不正な利用があった場合にはすぐにこれを発見する必要がある。このような処理をネットワークサービスの監視と称する。
【0003】ネットワークサービスとは、1つ以上のネットワーク接続された汎用電子計算機または専用電子計算機上で動作するプログラムの協調動作により実現されているアプリケーションを指す。ネットワークサービスの監視に関しては、
I. 監視のための標準が確立されていない。
II. アプリケーションを構成するプロセスが生成するログが唯一の情報源である。監視のための有益な情報を含んでいる可能性があるが、アプリケーション毎に独自に作られているため、統一性がない。
III. ログはマシン管理者が手作業で常時チェックしているか、あるいは管理者によってはチェックする作業を軽減するために解析プログラムを個別に開発し、これを用いている。というのが現状である。
【0004】
【発明が解決しようとする課題】上述したような従来のネットワークサービスの監視方法においては、監視対象となるサービスは一般に管理サイト毎に異なるとともに、また同じサービスの管理でも管理項目はサイト毎に異なるのが通常のことである。そして、例えば新しいサービスを導入する度に、または管理ポリシーが変更される度に、監視プログラムを記述し直す必要があり、管理者の負担を増大させるという問題がある。
【0005】また、従来のネットワークサービス監視方法では、マシン管理者がサービスに個別に対応することによって成り立っているため、管理のためのノウハウは管理者だけが持っており、熟練した管理者でない一般の利用者が管理を行うことはきわめて困難であるという問題がある。
【0006】更に、サービスが異なると管理手法も異なるため、管理の困難性を増す原因となっている。
【0007】また、サービスの不正利用などを迅速に検出し、これに対応するためには、サービスの利用状況に常に気を配る必要があり、またトラブルに素早く対応するためには、ログ情報を頻繁にチェックする必要があるが、これらも管理者にとっては大きな負担であるという問題がある。
【0008】本発明は、上記に鑑みてなされたもので、その目的とするところは、管理者の負担を軽減しながら異常状態を迅速に対応してネットワークサービスの監視を適確に行い得るネットワークサービス監視方法および装置とネットワークサービス監視プログラムを記録した

記録媒体を提供することにある。

【0009】

【課題を解決するための手段】上記目的を達成するため、請求項1記載の本発明は、電子メール、ネットニュース、WWWを含むネットワークサービスが提供されているネットワークに接続された電子計算機環境において、前記ネットワークサービスが生成するログ情報を逐次監視して、ログ情報の変化を検出し、ログ情報の解析手順をデータフロー図で記述して、監視プログラムを生成し、この生成した監視プログラムを配置し、前記ログ情報の変化を検出した場合、前記生成され配置された監視プログラムを実行し、これによりネットワークサービスを監視することを要旨とする。

【0010】請求項1記載の本発明にあっては、ログ情報の解析手順をデータフロー図で記述して、監視プログラムを生成し配置しておき、ネットワークサービスが生成するログ情報を逐次監視し、ログ情報の変化を検出した場合、監視プログラムを実行し、これによりネットワークサービスを監視するため、管理ポリシーの変化にも容易に対応できるとともに、管理者の負担を軽減しながら、異常時に迅速に対応することができる。

【0011】また、請求項2記載の本発明は、電子メール、ネットニュース、WWWを含むネットワークサービスが提供されているネットワークに接続された電子計算機環境において、前記ネットワークサービスが生成するログ情報を逐次監視して、ログ情報の変化を検出するログ情報変化検出手段と、ログ情報の解析手順をデータフロー図で記述して、監視プログラムを生成する生成手段と、この生成した監視プログラムを配置して記憶するデータベース手段と、前記ログ情報変化検出手段がログ情報の変化を検出した場合、前記データベース手段に記憶された監視プログラムを実行し、これによりネットワークサービスを監視する監視プログラム実行手段とを有することを要旨とする。

【0012】請求項2記載の本発明にあっては、ログ情報の解析手順をデータフロー図で記述して、監視プログラムを生成し配置しておき、ネットワークサービスが生成するログ情報を逐次監視し、ログ情報の変化を検出した場合、監視プログラムを実行し、これによりネットワークサービスを監視するため、管理ポリシーの変化にも容易に対応できるとともに、管理者の負担を軽減しながら、異常時に迅速に対応することができる。

【0013】更に、請求項3記載の本発明は、電子メール、ネットニュース、WWWを含むネットワークサービスが提供されているネットワークに接続された電子計算機環境において、前記ネットワークサービスが生成するログ情報を逐次監視し、ログ情報の変化を検出し、ログ情報の解析手順をデータフロー図で記述して、監視プログラムを生成し、この生成した監視プログラムを配置し、前記ログ情報の変化を検出した場合、前記生成され配置された監視プログラムを実行し、これによりネットワークサービスを監視するネットワークサービス監視プログラムを記録媒体に記録することを要旨とする。

【0014】請求項3記載の本発明にあっては、ログ情報の解析手順をデータフロー図で記述して、監視プログラムを生成し配置しておき、ネットワークサービスが生成するログ情報を逐次監視し、ログ情報の変化を検出した場合、監視プログラムを実行し、これによりネットワークサービスを監視するネットワークサービス監視プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0015】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。図1は、本発明の一実施形態に係るネットワークサービス監視装置の構成を示す図である。同図に示すネットワークサービス監視装置は、管理用ホスト1にそれぞれ設けられたものとして、管理者が管理しようとするサイトの管理ポリシーに合わせて、実行したいログ情報の解析手順であるログ情報に対する操作をデータフロー図で記述するデータフロー図（DFD：Data Flow diagram)エディタ11、該データフロー図エディタ11においてデータフロー図で記述されたログ情報の解析手順を実行するための監視プログラムを生成するトランスレータ13、該トランスレータ13で生成された監視プログラムを記憶するデータベース15、データベース15に記憶された監視プログラムを実行し、ネットワークサービスを監視する解析エージェント（AA：Analyzing Agent)17を有し、またサーバホスト3に設けられたものとして、管理用ホスト1のトランスレータ13で生成され、ネットワークを介して転送されて配置される監視プログラムを記憶するスクリプトデータベース(Script Database）15、該スクリプトデータベース15に記憶された監視プログラムを実行する解析エージェント（AA）17、サーバホスト3において管理したいネットワークサービスであるサービスアプリケーション（Service App.）が生成するログ情報を逐次監視し、ログ情報の更新等の変化を検出して通知する監視エージェント（RA：Retrieve Agent）19を有する。

【0016】更に詳しくは、データフロー図エディタ11は、利用者がログ情報に対する操作を予め準備されたノード部品の組み合わせにより図的記述で行うものである。このように図的記述を用いることにより、熟練した管理者だけでなく、予備知識のない一般利用者にも利用可能となる。

【0017】トランスレータ13は、利用者がデータフロー図により記述した管理ポリシーとしてのログ情報の解析手順を実行するためのプログラムを生成するためのサブシステムである。従来は管理者がプログラムを生成していたが、本実施形態では管理者はプログラムを記述

する手間を大幅に削減することができるようになる。

【００１８】スクリプトデータベース１５は、データフロー図エディタ１１により生成された監視プログラムを蓄積するサブシステムである。この蓄積された監視プログラムは必要に応じて解析エージェント（ＡＡ）１７により呼び出され、自動的に実行される。

【００１９】解析エージェント（ＡＡ）１７は、トランスレータ１３により生成された監視プログラムの実行をスケジューリングするためのエージェントである。利用者が記述したデータフロー図上の１つのノードは、トランスレータ１３により１つのプログラムへ自動変換される。この解析エージェント（ＡＡ）１７は、それぞれのプログラムの実行のタイミングを制御する機能を有する。

【００２０】各プログラムが起動される条件として、

（１）データ駆動的な実行規則に従いデータが揃った時点で実行する。

（２）予め与えられた一定時間間隔で実行する。

（３）利用者の指示のもとにオンデマンドで実行する。

の３つの方式の中からシステムにより選択される。解析エージェント（ＡＡ）１７は、監視エージェント（ＲＡ）１９からの通知により解析を実行するように起動され、これによりログ情報の更新されるタイミングでの解析の実行が可能となる。また、ログ情報の変化、すなわちサービスの状態の変化に合わせて監視プログラムを起動することができる。

【００２１】監視エージェント（ＲＡ）１９は、監視対象となるログ情報の更新状態を監視するためのエージェントである。利用者が指定した「必要な情報の鮮度」に基づいて収集期間を設定し、ログ情報を監視する。この監視エージェント（ＲＡ）１９が更新を検知した場合には、解析エージェント（ＡＡ）１７に通知するとともに、更新されたログ情報の内容を解析エージェント（ＡＡ）１７に転送する。この監視エージェント（ＲＡ）１９によりログに対するリアルタイムな解析が可能となり、サービスのトラブル発生に対して迅速な検出が可能となる。

【００２２】次に、図２を参照して、図１のネットワークサービス監視装置の作用について説明する。図２においては、まず（１）管理者は管理しようとするサイトの管理ポリシーに合わせて、実行したいログの解析手順をデータフロー図エディタ１１によりデータフロー図を用いて部品の組み合わせにより図的に記述する。次に、

（２）この図的に記述されたデータフロー図をトランスレータ１３により電子計算機上で実行可能な監視プログラムに変換し、更に実行させる必要のあるホスト、すなわち図１のサーバホスト３を判断し、このサーバホスト３に監視プログラムをネットワークを介して転送配置してスクリプトデータベース１５に記憶する。それから、監視したいネットワークサービスのプログラム（例えばメーササーバ等）が生成するログ情報を常に監視エージェント（ＲＡ）１９で監視して、該ログ情報の更新を迅速に検出する。（３）ログ情報の更新を迅速に検出すると、監視エージェント（ＲＡ）１９はこの検出結果をサーバホスト３および管理用ホスト１に通知し、この結果解析エージェント（ＡＡ）１７はスクリプトデータベース１５に記憶されている監視プログラムを実行し、サービスに関する情報を生成する。（４）この結果を管理者に対して電子メール、テキストファイル、グラフ、ページャ呼び出し等の指定された方法で通知する。

【００２３】次に、上記実施形態の具体例として、例えばＪａｖａによる実装について説明する。Ｊａｖａの特長の１つとしてＷＯＲＡ(Write Once Run Anywhere）が謳われており、動作環境を選ばないというメリットが得られる。また、トランスレータにより生成されるプログラムは、Ｐｅｒｌスクリプトを用いた。これは、ＯＳなどの実行環境に依存しないという特長を持つ。以上の２点から、この具体例では、高い可搬性を持つシステムが実現できている。

【００２４】各管理サイトで必要とされる管理項目や、管理対象となるサービスはそれぞれ異なる。このサイト間の差異およびサイトでの要求の変化に素早く追従できるようにするために、データフロー図の個々のノードをソフトウェアコンポーネント（ソフトウェア部品）で構築した。これにより、管理ポリシーなどの要求が変化した場合でも、コンポーネントを増減することだけによる素早い対応が可能となった。

【００２５】データフロー図エディタ上でのログ情報の指定には、正規表現を用いたログファイル名を指定する。これにより運用時の定期的なファイル名のローテートにも対応が可能となった。

【００２６】次に、この一実装例を用いたネットワークサービスの一例としてＤＨＣＰ(Dynamic Host Configuration Protocol）サーバの管理への適用例を示す。ＤＨＣＰサーバを管理するための管理項目の例としては、

（ａ）．不正アクセスの監視

（ｂ）．ＩＰアドレスの利用率の監視

の２つの機能が必要である。以下、本発明を用いて上記の３つの管理項目を管理する手順を示す。

【００２７】まず、図３に示すように利用者によって記述されたデータフロー図を参照して、登録利用者以外からの利用の検出、すなわち不正アクセスの監視について説明する。

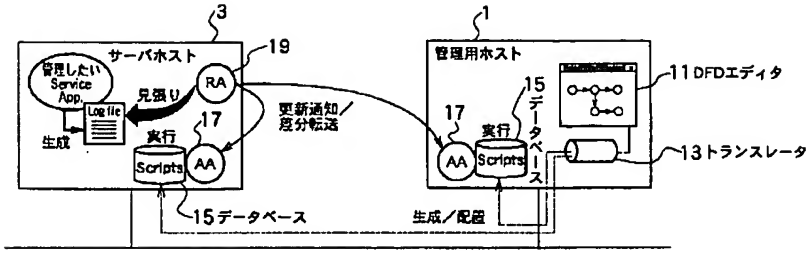
【００２８】ここで、記述された内容は、

１．ログ情報（Ｔ１）から、ＩＰアドレスのアサイン（割り当て）を示すレコードを取り出し（Ｔ３）、接続したネットワークインタフェースのＭＡＣアドレスを取り出す（Ｔ４）。

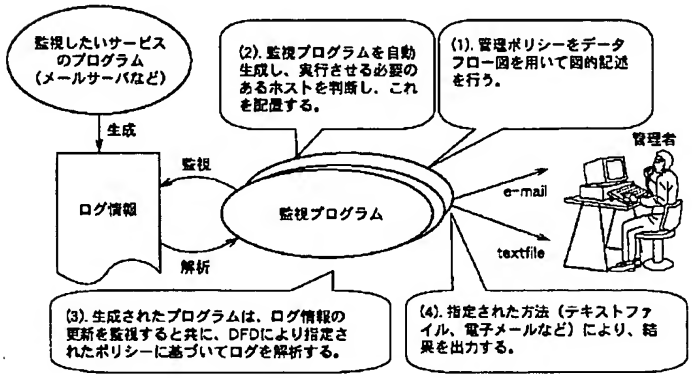
２．そのＩＰアドレスがアサインされたＭＡＣアドレスと、登録されている利用者のデータベース（Ｔ２）と結

合する（Ｔ５）。
３．登録されていないＭＡＣアドレスへアサインされたものを取り出し（Ｔ６）、これを管理者へ電子メールにより通知する。
という管理を行うものである。次に、この記述されたポリシーをトランスレータが実行可能プログラムへと変換し、スクリプトデータベースへ蓄積するとともに、監視エージェント、解析エージェントへと指令を出す。指令を受けた監視エージェントは、ログ情報の更新を見張り、解析エージェントがプログラムを実行する。
【００２９】次に、図４に示すように利用者によって記述されたデータフロー図を参照して、ＩＰアドレスの利用率の監視、すなわち割り当てられたＩＰアドレスの過不足の統計の作成について説明する。
【００３０】ここで、記述された内容は、
１．ログ情報（Ｔ１）から、ＩＰアドレスのアサイン（割り当て）およびリソース（返却）を示すレコードを取り出す（Ｔ２）。
２．接続を行った端末のネットワークインタフェースのＭＡＣアドレスを取り出す（Ｔ３）。
３．アドレスとアサインとリソースの組み合わせから状態を注する（Ｔ４）。
４．ＩＰアドレスの利用率を求め（Ｔ５）、管理者に通知する。
という管理を行うものである。次に、この記述されたポリシーをトランスレータが実行可能プログラムへと変換し、スクリプトデータベースへ蓄積するとともに、監視エージェント、解析エージェントへと指令を出す。指令を受けた監視エージェントは、ログ情報の更新を見張り、解析エージェントがプログラムを実行する。
【００３１】上述した実施形態では、管理用ホスト１のデータフロー図エディタ１１においてログ情報の解析手順をデータフロー図で記述し、この記述されたデータフロー図をトランスレータ１３で監視プログラムに生成し、この監視プログラムを管理用ホスト１のスクリプトデータベース１５に記憶するとともに、ネットワークを介してサーバホスト３に転送して配置してスクリプトデータベース１５に記憶する。それから、サーバホスト３の監視エージェント（ＲＡ）１９によりサーバホスト３のネットワークサービスが生成するログ情報を逐次監視し、ログ情報の変化を検出すると、解析エージェント（ＡＡ）１７に通知する。解析エージェント（ＡＡ）１７はこの監視エージェント（ＲＡ）１９から通知されたログ情報の変化の検出に応答し、スクリプトデータベース１５に記憶されている監視プログラムを実行し、これによりデータフロー図により指定されたポリシーに基づいてログを解析し、この結果をテキストファイル、電子メール等の指定された方法で出力し、管理者に通知する。
【００３２】この結果、管理者の有するノウハウをシステムとして実現でき、熟練した管理者でない一般の利用者による監視を支援することができる。また、ログ情報の更新を迅速に検出し、異常時に素早く対応できるように支援することができる。そして、ネットワーク管理者は管理ポリシーの変更に柔軟に対応することができ、またログ情報が更新されたことを監視し続ける必要がなくなり、更に異なるサービスを同一のインタフェースで管理することができるようになる。
【００３３】
【発明の効果】以上説明したように、本発明によれば、ログ情報の解析手順をデータフロー図で記述して、監視プログラムを生成し配置しておき、ネットワークサービスが生成するログ情報を逐次監視し、ログ情報の変化を検出した場合、監視プログラムを実行し、これによりネットワークサービスを監視するので、管理ポリシーの変化にも容易かつ迅速に対応できるとともに、管理者はログ情報の変化を常に監視する必要がなくなり、これにより管理者の負担を大幅に軽減し、異常時に迅速に対応することができる。
【図面の簡単な説明】
【図１】本発明の一実施形態に係るネットワークサービス監視装置の構成を示す図である。
【図２】図１に示すネットワークサービス監視装置の原理を示す説明図である。
【図３】図１のネットワークサービス監視装置の適用例としてＤＨＣＰサーバ管理における登録利用者以外からの利用の検出を示すデータフロー図である。
【図４】図１のネットワークサービス監視装置の別の適用例としてＤＨＣＰサーバにおける割り当てられたＩＰアドレスの過不足の統計の作成を示すデータフロー図である。
【符号の説明】
１　管理用ホスト
３　サーバホスト
１１　データフロー図エディタ
１３　トランスレータ
１５　スクリプトデータベース
１７　解析エージェント（ＡＡ）
１９　監視エージェント（ＲＡ）

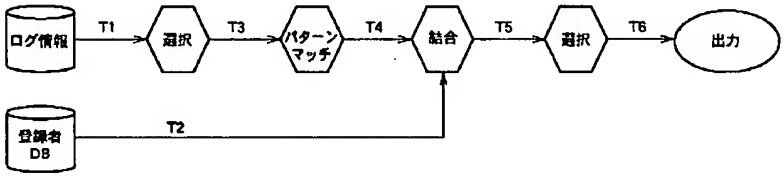
【図1】


3
サーバホスト
管理したい Service App.
Log file
生成
RA
19
見張り
17
実行
Scripts
AA
更新通知/差分転送
15データベース
1
管理用ホスト
11 DFDエディタ
15データベース
17
実行
AA
Scripts
13トランスレータ
生成/配置

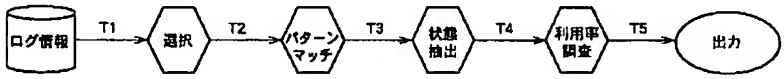
【図2】


監視したいサービスのプログラム(メールサーバなど)
生成
ログ情報
監視
解析
監視プログラム
(2). 監視プログラムを自動生成し、実行させる必要のあるホストを判断し、これを配置する。
(1). 管理ポリシーをデータフロー図を用いて図的記述を行う。
管理者
e-mail
textfile
(3). 生成されたプログラムは、ログ情報の更新を監視すると共に、DFDにより指定されたポリシーに基づいてログを解析する。
(4). 指定された方法(テキストファイル、電子メールなど)により、結果を出力する。

【図3】


ログ情報
T1
選択
T3
パターンマッチ
T4
結合
T5
選択
T6
出力
登録者DB
T2

【図4】


ログ情報
T1
選択
T2
パターンマッチ
T3
状態抽出
T4
利用率調査
T5
出力